Zscaler Cellular

Secure IoT and mobile device traffic with seamless global connectivity, visibility, and control, built for scalable and efficient enterprise operations

DATASHEET

Overview

The surge in IoT and cellular devices is boosting productivity—but it's also creating security gaps that legacy solutions can't address. Default credentials, unpatched vulnerabilities, and limited visibility leave IoT assets exposed to attacks and rogue activities. An expanded attack surface invites undetected threats, while inefficient backhauling and fragmented global coverage add complexity and cost. Without granular access controls, attackers can move laterally across your environment.

Zscaler Cellular redefines IoT security—delivering the scalable, zero trust protection and seamless connectivity enterprises need. It's not just about connecting billions of devices—it's about securing every connection.

Business Values

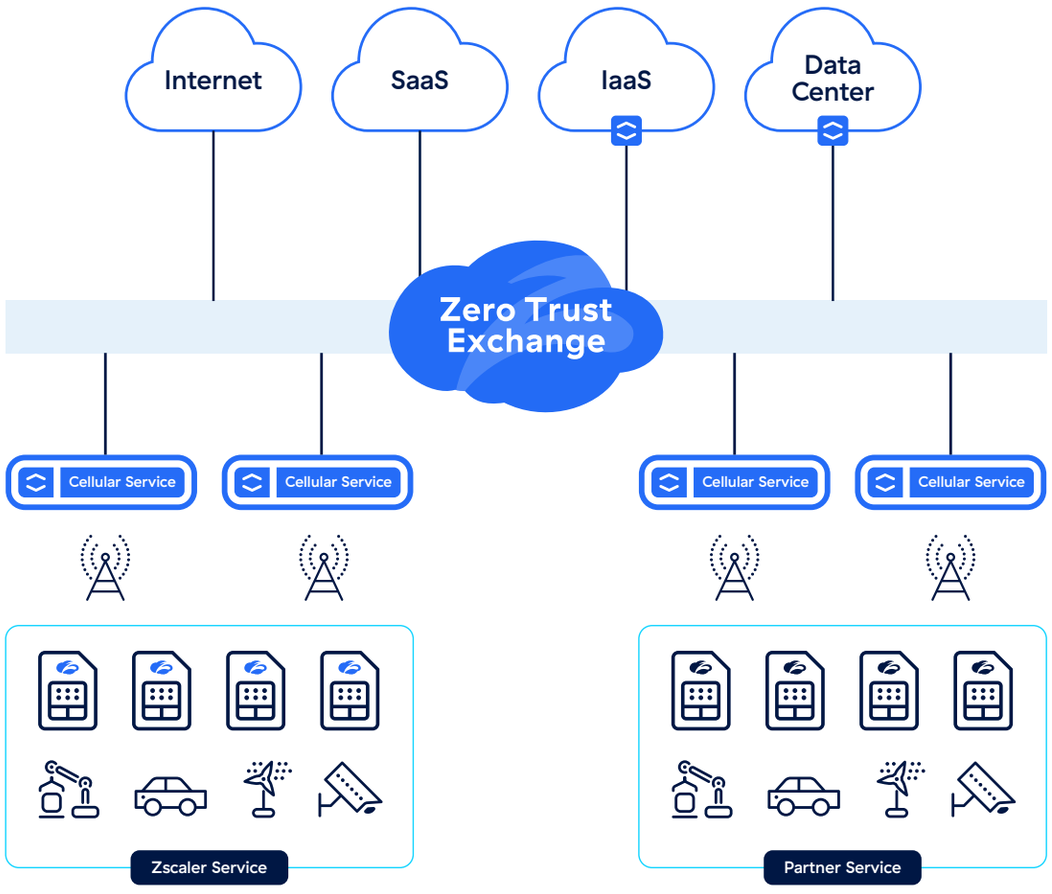
Instant Connectivity
Plug and play deployment model– just "Enable SIM and GO"

Global Reach
Secured service spanning 520+ carrier networks worldwide

Invisible to attackers
No routable network, no attack surface

Total Oversight
Full Visibility, granular Control and deep threat Protection

Zero Trust Access
Remote access by design—secure every device, everywhere



Zscaler Service

Zscaler provides an end-to-end service for the customer. Zscaler provides the SIM, Cellular path and connectivity to the Zscaler Zero Trust Exchange

Partner Service

Joint solution with partner MNO/MVNO. Partner provides the SIMs and Cellular path. Zscaler provides the onramp tot he Zscaler Zero Trust Exchange

7.2B[1]

Cellular IoT connections by 2029 (from 3.9B in 2023)

40B+[2]

connected IoT devices worldwide by 2030 (IoT Analytics)

$790B+[3]

spend on connected devices by 2028

Zscaler Cellular: Redefining Security and Connectivity for IoT and Mobile Devices

Zscaler Cellular is a transformative solution designed to secure and simplify connectivity for cellular-connected IoT and mobile devices using a Zero Trust architecture. By leveraging the Zscaler Zero Trust Exchange (ZTE), it extends industry-leading Zero Trust principles into the cellular domain, offering secure, scalable, and efficient connectivity for IoT ecosystems and mobile deployments. This comprehensive solution directly addresses the challenges of securing billions of cellular-connected endpoints—especially in environments where traditional tools like VPNs and firewalls struggle to scale. Zscaler Cellular seamlessly integrates into existing telecom infrastructures to deliver an unmatched combination of security, visibility, and operational simplicity.

Zscaler Cellular solved our long-standing challenge: how to effectively secure the IoT and mobile devices that we deploy at clients' and customers' properties," said Brian Shelby, Director of IT Infrastructure and Cybersecurity at Maverick Transportation. "We need to operate these tablets, time-tracking devices, and more on sites where we have no control over the networking options provided or the operating environment, and without adding software agents or using remote access VPNs. The solution allowed us to create device-bound authentication through Zscaler. This became our test case, and after equipping kiosks with Zscaler Cellular, our Zero Trust policies are enforced through the Zscaler Cellular Edge. The lines are gone, the employee experience is better, our business is still protected, and we don't need a software agent or VPN on the device.

BRIAN SHELBY
Director of Infrastructure & Security

ONE MISSION, TWO PATHS: ZSCALER CELLULAR SECURITY TAILORED FOR EVERY NEED

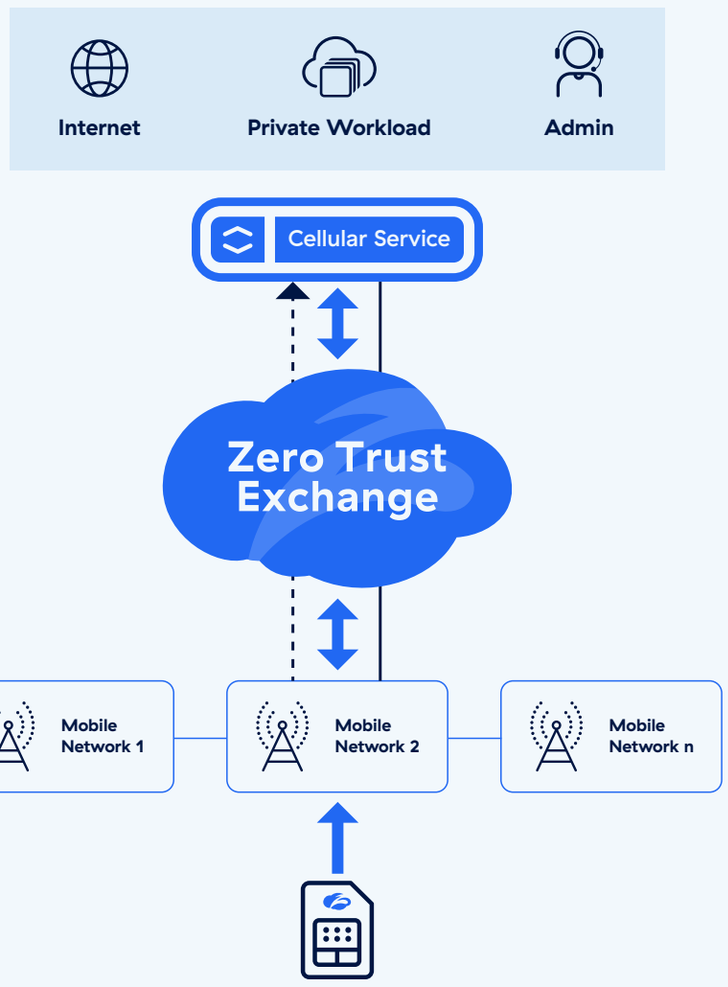
Zscaler offers two deployment paths to secure every cellular IoT device—ensuring seamless zero trust protection, comprehensive visibility, and operational simplicity, no matter your architecture.

Both options securely route cellular traffic to the Zscaler Zero Trust Exchange for inspection, policy enforcement, and actionable insights—giving you the flexibility to choose the fit that best matches your operational and management needs. Below, explore the technical specifications to see what's included and excluded in each approach.

ZSCALER CELLULAR SERVICE:

A turnkey, plug-and-play solution using Zscaler SIMs for instant, secure connectivity across vending machines, EV chargers, kiosks, and more. Enjoy agentless zero trust segmentation, granular policies, advanced threat protection, and detailed telemetry for real-time monitoring and anomaly detection—all delivered end-to-end by Zscaler.

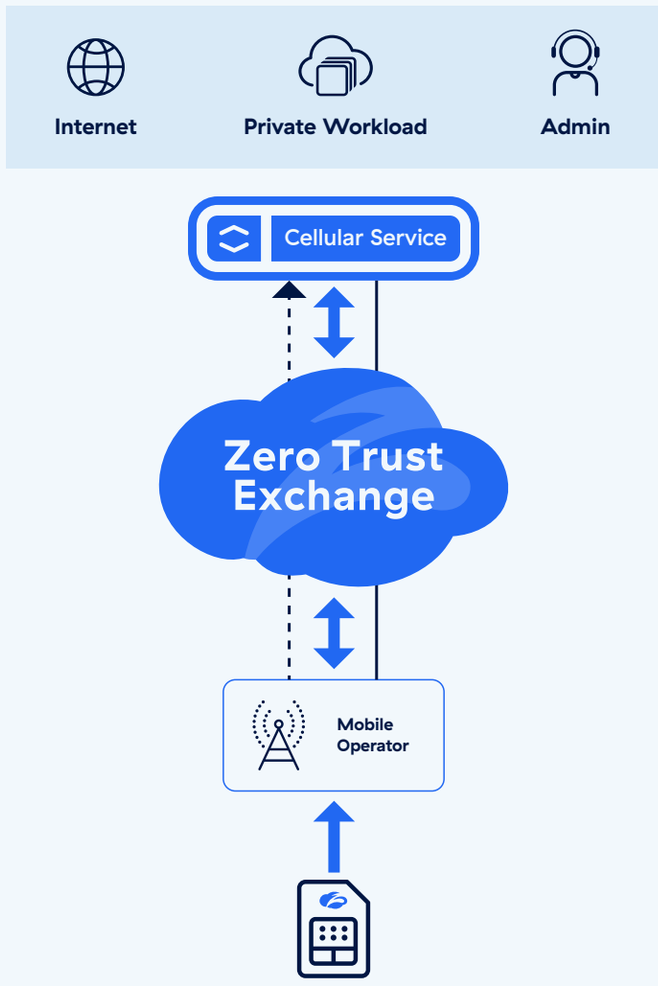
Zscaler Cellular



ZSCALER CELLULAR PARTNER SERVICE

Integrates with any mobile provider's SIMs and infrastructure, offering effortless "on-ramp" connectivity to the Zscaler platform. No endpoint reconfiguration required. Managed by Zscaler or your mobile partner, this approach ensures bidirectional security, high availability with failover, and robust telemetry for analytics and reporting.

Zscaler Cellular Partner



CATEGORY	FEATURE	ZSCALER CELLULAR SERVICE	ZSCALER CELLULAR PARTNER SERVICE
Security & Control	Full Bi-Directional Access using ZTE	✓	⚠ (depends on partner deployment)
	Zero Trust Integration	✓	✓
	Geo Controls	✓	⚠ (dependent on partner capabilities)
	Anomaly Detection	✓	⚠ (integrated if partner supports)
Monitoring & Visibility	Logging and Network Event Access	✓	⚠ (dependent on partner infrastructure)
	Granular Policy Enforcement	✓	✓
	ZDX Monitoring	✓	✓
Connectivity	Cellular Network Resilience / Failover	✓	✗ (Feature is unavailable in the service)
	Global Roaming	✓	⚠ (availability subject to partner)
Management	SIM Orchestration	✓	⚠ (managed if partner supports SIM integration)
	Zero Trust Remote Access	✓	⚠ (partner-managed SIM deployment required)

✓ **Included:** Feature is fully supported within the service.
⚠ **Conditional:** Feature availability depends on the capabilities or deployment architecture managed by the service partner.

Key Use Cases

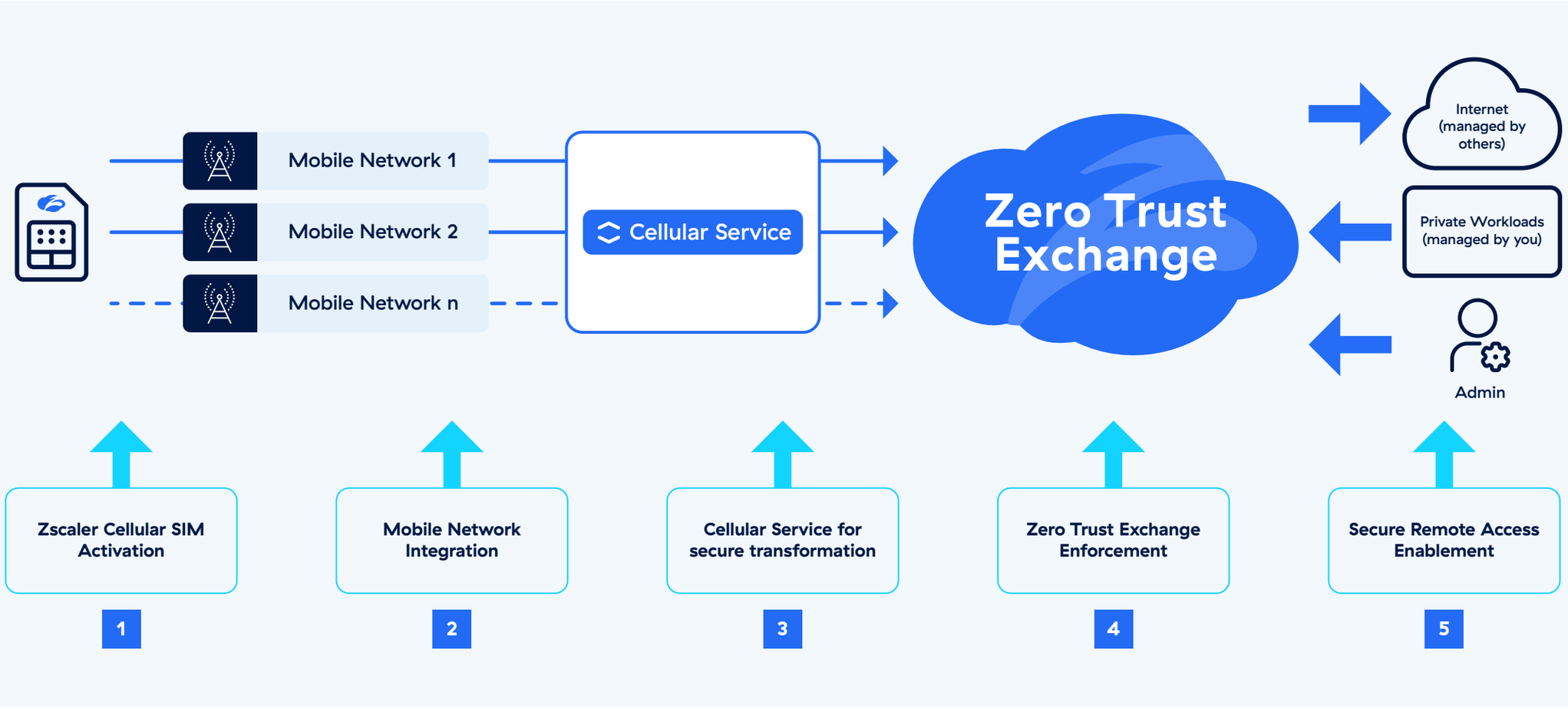
USE CASES	DESCRIPTION	APPLICABLE FOR INDUSTRIES	DEPLOYED IN
Secure ERP transactions	• No software installation • One, simple deployment • Install SIM • Connection goes over mobile network • Zscaler Zero Trust Policy is applied for » Private workloads » Secure local Internet	• Transport • Energy • Automotive • Logistics/ Shopping • Manufacturing	A global leading biopharmaceutical company A multinational manufacturer of fluid handling solutions
Resilient Signaling	• Ensure real time data • Over any available carrier network • Fail over to next network, when primary is not available • No loss of connection or data • Secure access to private application	• Transport • Energy • Automotive • Logistics/ Shopping • Manufacturing	A renowned consulting and engineering firm specializing in structural and architectural diagnostics
Zero Trust access to SIM devices	• Secure Access to Devices • Resilient & Secure path into your devices » No reliance on dedicated network » Only your authorized initiators can access » Control access by identity, not network » Works over any mobile network	• Transport • Energy • Automotive • Logistics/ Shopping • Manufacturing	An international engineering group specializing in mining and materials technology
Zero Trust Access for Out-of-band (OOB) access	• Secure Out of Band Access • Deliver Protected & Granular Access » To critical services » Authorized access only » Leverage to return function to critical infrastructure » Works over any mobile network	• Transport • Energy • Automotive • Logistics/ Shopping • Manufacturing	A leading global professional services and consulting firm

How does Zscaler Cellular work?

Zscaler Cellular works by seamlessly uniting the mobile networks with zero trust. This is achieved by leveraging the power, breadth and simplicity of connecting to a mobile network and tying this directly into the use of the Zero Trust Exchange from Zscaler.

Zscaler has done this by integrating a secure zero trust gateway service between the initiating SIM and the rest of the world. Allowing for the SIM to seamlessly roam, yet maintain connectivity directly to its local Zero Trust Exchange. And this is achieved without installing any software on the device

This simplicity of use, all whilst ensuring complete visibility, control and protection, allows for the end customer to have their mobile connected devices operate under complete zero trust control.



Zscaler Cellular enables secure connectivity for customer devices using Zero Trust principles. Each customer is assigned their own Zscaler Cellular Service, which is provisioned based on their requirements with the following components:

1. **Zscaler Cellular SIM Activation**
   Each customer receives unique Zscaler Cellular SIMs that are securely generated and allocated. These SIMs are tied (“pinned”) to the customer’s Zero Trust policy through their Zscaler Cellular Service. Each SIM is equipped with a unique identifier, which links it to a corresponding Zscaler tenant location and sublocation for seamless policy creation and management.

2. **Mobile Network Integration**
   At the customer’s request, Zscaler Cellular SIMs are configured to operate across specified mobile networks worldwide. When a SIM connects to networks from the approved list (within allowed regions), the local mobile network operator receives traffic from the SIM and allows its transmission to predefined destinations. In a Zscaler Cellular setup, this destination is always the secure Zscaler Cellular Service.

3. **Zscaler Cellular Service for Secure Transmission**
   The Zscaler Cellular Service functions as a gateway, receiving and managing traffic from the mobile network operators. Based on customer requirements, this service can be deployed globally, regionally, or locally to ensure optimal routing and performance for SIM-initiated traffic. The Zscaler Cellular Service guarantees that all traffic is securely forwarded to the customer's defined Zero Trust policy.

4. **Zero Trust Exchange Enforcement**
   Once traffic reaches the Zero Trust Exchange, the customer's configured policies are applied. These policies direct traffic toward appropriate controls, steering functions, and destinations, whether reaching the internet or private workloads. This ensures consistent zero trust enforcement for all traffic originating from customer SIMs.

5. **Secure Remote Access Enablement**
   The Zero Trust Exchange facilitates secure remote access for customer devices originating from the SIMs, maintaining zero attack surface. Granular control is enabled to enforce Zero Trust principles for users accessing workloads, applications, or systems—whether within private environments or over the internet.

Key Differentiators

- **Zero Trust Security at Every Layer:** Zscaler Cellular brings comprehensive Zero Trust controls to cellular-connected devices, with features like device locking, tagging, and anomaly detection. Both agentless and agent-based remote access, as well as privileged access management, ensure secure connections without increasing complexity. Cloud-delivered security services, including DNS filtering, SWG, firewall, and ZTNA, guard every device—eliminating external attack surfaces and blocking lateral movement.

- **Simplified Operations and Lower Cost:** With a Network-as-a-Service approach and direct-to-cloud routing, Zscaler Cellular removes the need for traditional circuits, firewalls, or VPNs. Global coverage is handled under a single contract, and cloud-based segmentation replaces complex hardware, reducing both management overhead and overall cost.

- **Reliable, Global Connectivity:** Connecting across 185+ countries and 515 carriers, Zscaler Cellular delivers resilient service and regional egress to minimize latency. Modern SIM technology supports rapid, over-the-air updates and deployments, ensuring always-on, adaptive connectivity for all devices.

Zscaler Cellular Benefits

COMPREHENSIVE SECURITY AND CONTROL

Unmatched protection, granular access, and real-time visibility for all cellular endpoints—delivered from the cloud

RELIABLE, HIGH-PERFORMANCE COVERAGE

Seamless, resilient connectivity in 180+ countries, low latency, rapid deployment, and always-on updates with advanced SIM technology

LOWER CONNECTIVITY COSTS

Eliminate circuits, VPNs, and firewalls—streamline global coverage with a single, unified contract

SEAMLESS, ZERO-TOUCH MANAGEMENT

Automated, zero-touch provisioning for effortless deployment and security—connect every cellular device out of the box

[1] IoT connections outlook – Ericsson

[2] Gartner's Internet of Things, Endpoints and Communications, Worldwide, 2022–2032, 1Q25 Update

[3] Gartner's IoT Market Opportunity by Technology Segment Forecast (2022–2028)

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Zero Trust Everywhere